

AD-A128 418

ERROR-FREE PARALLEL HIGH-ORDER CONVERGENT ITERATIVE
MATRIX INVERSION BASE..(U) MARYLAND UNIV COLLEGE PARK
COMPUTER VISION LAB E V KRISHNAMURTHY NOV 82 TR-1229

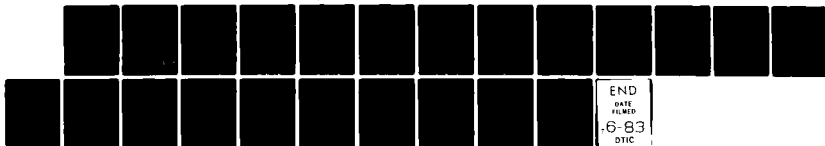
1/1

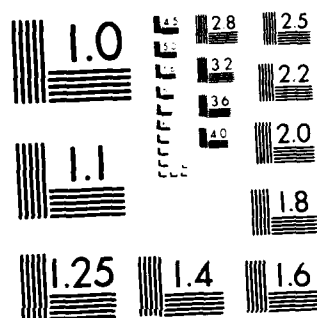
UNCLASSIFIED

AFOSR-TR-83-0387 AFOSR-77-3271

F/G 12/1

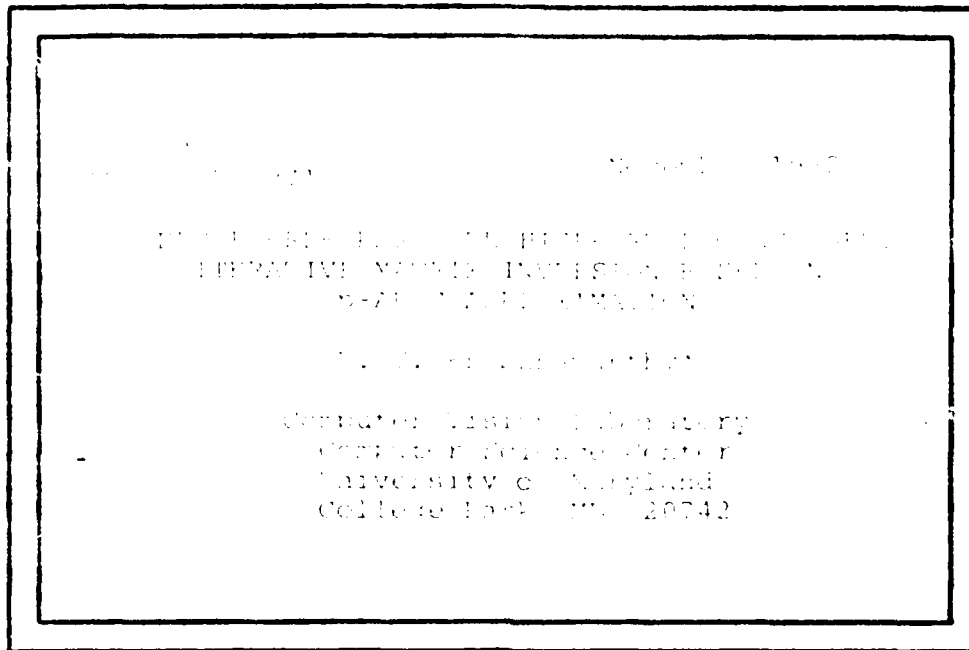
NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

12 A 128418



COMPUTER SCIENCE
TECHNICAL REPORT SERIES



UNIVERSITY OF MARYLAND
COLLEGE PARK, MARYLAND
20742

DTIC FILE COPY

DTIC
ELECTE
MAY 23 1983
S E D

83 05 21 063

Approved for public release
distribution unlimited,

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER AFOSR-TR- 83 - 0387	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) ERROR-FREE PARALLEL HIGH-ORDER CONVERGENT ITERATIVE MATRIX INVERSION BASED ON p-ADIC APPROXIMATION		5. TYPE OF REPORT & PERIOD COVERED TECHNICAL
7. AUTHOR(s) E.V. Krishnamurthy		6. PERFORMING ORG. REPORT NUMBER TR-1229
9. PERFORMING ORGANIZATION NAME AND ADDRESS Department of Computer Science University of Maryland College Park MD 20742		8. CONTRACT OR GRANT NUMBER(s) AFOSR-77-3271
11. CONTROLLING OFFICE NAME AND ADDRESS Mathematical & Information Sciences Directorate Air Force Office of Scientific Research Bolling AFB DC 20332		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS PE61102F; 2304/A2
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		12. REPORT DATE NOV 82
		13. NUMBER OF PAGES 18
		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited.		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Parallel computation; matrix inversion; p-adic approximation.		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) The Newton-Schultz iterative scheme is reformulated in an algebraic setting to compute the exact inverse of a matrix (or the solution of a linear system of equations) over the ring of integers, with a high order of convergence, by using a finite segment p-adic representation of a rational. This method is divergence-free; it starts with the inverse of a given matrix over a finite field (called the priming step) and then iterates successively to construct, in parallel, the p-adic approximants (Hensel Codes) of the rational elements of the inverse matrix. The p-adic approximant is then converted back (CONTINUED)		

DD FORM 1 JAN 73 1473

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

ITEM #20, CONTINUED: to the equivalent rational using the extended Euclidean algorithm.

The method involves only parallel matrix multiplications and complementations and has a quadratic convergence rate. Extension to achieve higher order convergence is straightforward if parallel matrix arithmetic facilities for higher precision operands (in a prime base system) are available.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

③

AIR FORCE OFFICE OF SCIENTIFIC RESEARCH (AFOSR)
NOTICE OF FINAL REPORT TO DTIC
This technical report has been approved and is
approved for public release under E.O. 13526-12.
Distribution is unlimited.
MATTHEW J. FLEMMING
Chief, Technical Information Division

TR-1229
AFOSR-77-3271

November 1982

ERROR-FREE PARALLEL HIGH-ORDER CONVERGENT
ITERATIVE MATRIX INVERSION BASED ON
p-ADIC APPROXIMATION

E. V. Krishnamurthy*

Computer Vision Laboratory
Computer Science Center
University of Maryland
College Park, MD 20742

ABSTRACT

↙ The Newton-Schultz iterative scheme is reformulated in an algebraic setting to compute the exact inverse of a matrix (or the solution of a linear system of equations) over the ring of integers, with a high order of convergence, by using a finite segment p-adic representation of a rational. This method is divergence-free; it starts with the inverse of a given matrix over a finite field (called the priming step) and then iterates successively to construct, in parallel, the p-adic approximants (Hensel Codes) of the rational elements of the inverse matrix. The p-adic approximant is then converted back to the equivalent rational using the extended Euclidean algorithm.

The method involves only parallel matrix multiplications and complementations and has a quadratic convergence rate. Extension to achieve higher order convergence is straightforward if parallel matrix arithmetic facilities for higher precision operands (in a prime base system) are available. ↗

*Permanent address: Indian Institute of Science, Bangalore - 560012, INDIA

The support of the U.S. Air Force Office of Scientific Research under Grant AFOSR-77-3271 is gratefully acknowledged, as is the help of Janet Salzman in preparing this paper.

83 05 23.063

1. Introduction

Error-free direct methods for the inversion of numerical and polynomial matrices are available in the literature [1] [2]. In this paper we describe a parallel error-free high-order convergent matrix inversion method for matrices over integers, based on the Newton-Schultz iterative scheme [3] [4] and the p-adic approximation [5-9]. Some of the important aspects of this scheme are:

- (i) Inversion of matrices over p-adic fields, analogously to inverting or reciprocating the numbers, without any convergence problem.
- (ii) The exact and simultaneous determination of the rational elements of the inverse matrix in p-adic digit parallel fashion with a quadratic or higher rate.
- (iii) Easy realization of the scheme and its variants (higher-order convergent extensions) by parallel matrix multiplications.

This paper is organized in seven sections. In the second section we outline the principle of the Newton-Schultz scheme for reciprocating numbers. The third section describes the reformulation of the Newton-Schultz scheme in an algebraic setting to compute the p-adic approximant to the inverse of a matrix over the ring of integers. In the fourth section we describe the extended Euclidean algorithm that converts a given p-adic approximant over a range of rationals into an equivalent rational. The fifth section contains an example.

In Section 6 we briefly deal with the solution of a linear system of equations, having a linear convergence rate. Several remarks pertaining to possible extensions and generalizations are provided in the last section.

2. The principle

Let $f(x)$ be a real function of the real variable x and $x=\alpha$ be a root of $f(x)=0$. We assume that:

- (a) $f(x)$, $f'(x)$ and $f''(x)$ are continuous in a neighborhood $[a,b]$ of $x=\alpha$; (b) $x=\alpha$ is an isolated root in $[a,b]$; (c) $f'(x)$ and $f''(x)$ do not vanish in $[a,b]$.

The search for the root $x=\alpha$ entails finding the root of the equation

$$x = x - \frac{f(x)}{f'(x)} = \phi(x).$$

Since $\phi'(\alpha)=0$ there exists a neighborhood of $x=\alpha$ such that the sequence $\{x_i\}_{i=0}^{\infty}$ defined by

$$x_n = x_{n-1} - f(x_{n-1})/f'(x_{n-1}) \quad (n=1,2,\dots) \quad (1)$$

converges to $x=\alpha$ if the first approximation $x=x_0$ lies in this neighborhood. Applied to the function $f(x)=1/x-a$ (1) gives the Newton-Schultz scheme

$$x_n = x_{n-1}(2-ax_{n-1}) \quad (2)$$

The sequence (2) converges to a^{-1} . The matrix inversion algorithm to be described in the next section is by analogy based on the sequence of iterates defined by (2) [3] [4].

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
21

3. The Newton-Schultz method

Let $A=[a_{ij}]$ be a matrix over the ring of integers Z and p a prime such that $\det A \bmod p \neq 0$. (The reason for this will become clear later.) The algorithm first constructs $A^{-1} \bmod p$ and using this in the Newton-Schultz recurrence obtains a segmented p -adic representation of the inverse matrix [5-9].

Theorem 1: There exists a matrix sequence $\{B_{2^i}\}_{i \geq 0}$ such that $AB_{2^i} \bmod p^{2^i} = I$ for all $i \geq 0$, where A is the matrix to be inverted and I is the identity matrix; B_{2^i} is the inverse of A (in Z) $\bmod p^{2^i}$ (or B_{2^i} is the p -adic approximant of A^{-1}).

Proof: We show the sequence $\{B_{2^i}\}_{i \geq 0}$ can be generated recursively and then prove by induction that it has the property stated, namely, $AB_{2^i} \bmod p^{2^i} = I$. The first member of the sequence B_1 is obtained in a priming step by solving

$$AB_1 \bmod p = I$$

by Gaussian elimination or some other method. It amounts to finding the inverse of A in $Z \bmod p$. Then in a powering step we use the recurrence relation

$$B_{2^i} = B_{2^{i-1}} (2I - AB_{2^{i-1}}) \bmod p^{2^i} \quad (i \geq 1) \quad (3)$$

to construct the successive iterates.

To see that the theorem holds let $AB_{2^i} \bmod p^{2^i} = I$ be true for $i = n-1$ ($n \geq 1$); then, by (3)

$$(AB_{2^n}) \bmod p^{2^n} = AB_{2^{n-1}} (2I - AB_{2^{n-1}}) \bmod p^{2^n}$$

Since $AB_{2^{n-1}} \bmod p^{2^{n-1}} = I$ by the induction hypothesis, we have

$$AB_{2^{n-1}} = I + p^{2^{n-1}} E_{n-1},$$

where E_{n-1} is the error matrix. Thus we can write

$$AB_{2^n} \bmod p^{2^n} = (I + p^{2^{n-1}} E_{n-1})(I - p^{2^{n-1}} E_{n-1}) \bmod p^{2^n}.$$

Since by construction the theorem holds for $n=0$, it is true for all $n \geq 0$ by induction.

Our algorithm first obtains B_{2^k} by iterating k times, where k is the minimum integer satisfying the inequality

$$\sqrt{\frac{p^{2^k} - 1}{2}} \geq \prod_{i=1}^n \left(\sum_{j=1}^n a_{ij}^2 \right)^{1/2} \quad (4)$$

This inequality ensures that the largest element of the inverse matrix lies within the range of the segmented p -adic representation of the corresponding rational [5] [8].

Let N denote a positive integer satisfying the inequality

$$N \leq \sqrt{\frac{p^{2^k} - 1}{2}} \quad (5)$$

We define a finite subset F_N of the rational numbers Q as the set

$$F_N = \left\{ \alpha = \frac{c}{d}; 0 \leq |c| \leq N \text{ and } 0 \leq |d| \leq N \right\}$$

We call the set F_N the order N Farey fractions, or simply Farey rationals of order N .

If p and k are properly chosen to satisfy (4) then the rationals F_N which are mapped onto their segmented p -adic representations in B_{2^k} can be uniquely recovered using an algorithm which is based on the extended Euclidean algorithm for finding the greatest common divisor of two integers [10] [11].

Let a/b and w be the ij -th entry of A^{-1} and B_2^k respectively.

Then

$$ab^{-1} \bmod p^{2^k} = w \quad (6)$$

since b^{-1} exists $\bmod p^{2^k}$, due to the fact that $\det A \bmod p \neq 0$.

In the following section we describe how to recover a/b given w , provided (4) is satisfied. This algorithm filters out a very small subset of rationals among which the desired rational belonging to F_N occurs. We will call the function that computes a/b given w , the EUCLID; thus $\text{EUCLID}(w) = a/b$.

Remark

The number k determined from (4) is generally larger than desired; so to iterate k times entails much superfluous computation. A practical method of avoiding this would be to compute $\text{EUCLID}(B_2^k)$ and $\text{EUCLID}(B_2^{k+1})$ starting with some reasonable k and stop as soon as they are equal. This would unambiguously determine the inverse.

4. Computation of Farey rationals using the Euclidean algorithm

The Euclidean algorithm [11] constructs three pairs of numbers (u_i, u'_i) , (a_i, b_i) , (t_i, t'_i) for each $i=0,1,2,\dots,k$ starting with $u_0=p^r, u'_0=0$, $a_0=w, b_0=1$ and ending when $t_k=0$, as illustrated in Table 1; here the symbol $[]$ denotes the lower integral part

Note that the q_i 's here correspond to the continued fraction expansion [5] [12] of p^r/w .

It can easily be shown that the pairs (a_i, b_i) in Table 1 satisfy the following conditions [10] [11]:

Cross-product rule:

$$|a_i \cdot b_{i+1}| + |a_{i+1} \cdot b_i| = p^r \leq 2N^2 + 1$$

Monotonicity:

$$|a_{i+1}| \leq |a_i|, \text{ with } a_0=w, a_k=1 \quad (8)$$

$$|b_{i+1}| \geq |b_i| \text{ with } b_0=1, b_k=w^{-1} \pmod{p^r} \quad (9)$$

where w is such that $\gcd(w, p^r)=1$ and w^{-1} denotes the multiplicative inverse of $w \pmod{p^r}$.

It is now necessary to show that (i) there exists a pair (a_j, b_j) in Table 1 which satisfies the condition of a Farey rational F_N (Section 3), and (ii), such a pair is unique in the sense that there exists no other pair belonging to F_N .

To prove this, we use the fact that a_i (starting with $a_0=w$) successively decreases to 1; and b_i (starting with $b_0=1$) successively increases to w^{-1} when $\gcd(w, p^r) = 1$.

Let us assume that for some j , b_j has already increased from 1 to $|N'|$ with $|N'| \leq |N|$ and is close to $|N|$, and the corresponding a_j has already decreased from w to $|N''|$ where $|N''| > |N|$ and

is close to $|N|$. Then using (7) we can prove that the succeeding pair (a_{j+1}, b_{j+1}) will have to be in F_N or in other words a pair of the form (a_{j+1}, b_{j+1}) with $|a_{j+1}| \leq N$ and $|b_{j+1}| > N$ which skips a Farey rational belonging to F_N cannot exist.

For if $|a_j| \geq N+1$ and $|b_j| \leq N$ and $|a_{j+1}| \leq N$ and $|b_{j+1}| \geq N+1$, we have $|a_{j+1} \cdot b_j| \leq N^2$. Using this in (7) we obtain $|a_j \cdot b_{j+1}| \geq N^2 + 1$. But we have $|a_j| \geq N+1$. Therefore $|b_{j+1}| \leq (N^2 + 1)/(N+1) = [N]$. Hence our assumption $|b_{j+1}| > N$ is false.

We will now show that there is only one such rational belonging to F_N . In other words, we will show that if for some j , (a_j/b_j) belongs to F_N then (a_{j+1}/b_{j+1}) cannot be in F_N . Note that the cross-product is maximum when

$$\begin{aligned} |a_j| &= N, \quad |b_j| = N - 1 \\ |a_{j+1}| &= N-1, \quad |b_{j+1}| = N. \end{aligned}$$

In such a case

$$|a_j \cdot b_{j+1}| + |b_j \cdot a_{j+1}| = (N-1)^2 + N^2 < 2N^2 + 1$$

would still be short of satisfying (7). Notice that for any other choice of $a_j, b_j, a_{j+1}, b_{j+1}$ the condition (7) would be more severely violated. Also when $|a_j| = |b_j| = N$, it is not possible for $|a_{j+1}| = N$, since a_{j+1} would become zero by the algorithm in Table 1.

Thus a p-adic approximant (Hensel Code [5]) with the weight w corresponds to the rational a_j/b_j belonging to F_N and the conversion is complete.

Remarks

- (i) The class of rationals generated by the above algorithm may contain a rational (in non-reduced form) whose reduced

form is in F_N ; but this is an invalid choice. (See example.)

- (ii) If $\gcd(w, p^r) \neq 1$, the factor is taken out and the result adjusted suitably.

Example

Let $p=5$, $r=4$, and $w=448$. Hence $N \leq 17$. We now show in Table 2 the computations corresponding to Table 1 of the algorithm. The Farey rational is $11/7$ (and not $5/60$).

5. Matrix-inversion example

$$\text{Let } A = \begin{bmatrix} 1 & -1 & 2 \\ 3 & 2 & 4 \\ 0 & 1 & -2 \end{bmatrix}$$

Let $p = 3$:

$$[A]_3 = \begin{bmatrix} 1 & 2 & 2 \\ 0 & 2 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 2 & 2 \end{bmatrix} \pmod{3}$$

$$B_2 = \begin{bmatrix} 1 & 0 & 1 \\ 6 & 7 & 2 \\ 3 & 8 & 5 \end{bmatrix} \pmod{3^2=9}$$

$$B_4 = \begin{bmatrix} 1 & 0 & 1 \\ 60 & 61 & 20 \\ 30 & 71 & 50 \end{bmatrix} \pmod{3^4=81}$$

$$B_8 = \begin{bmatrix} 1 & 0 & 1 \\ 4920 & 4921 & 1640 \\ 2460 & 5741 & 4100 \end{bmatrix} \pmod{3^8=6561}$$

$$B_{16} = \begin{bmatrix} 1 & 0 & 1 \\ 32285040 & 32285041 & 10761680 \\ 16142520 & 37665881 & 26904200 \end{bmatrix} \pmod{3^{16}=43046721}$$

We find that

$$\text{EUCLID}(B_{16}) = \begin{bmatrix} 1 & 0 & 1 \\ -3/4 & 1/4 & -1/4 \\ -3/8 & 1/8 & -5/8 \end{bmatrix} = \text{EUCLID}(B_8) = A^{-1}$$

Note that the inverse matrix elements are simultaneously determined in p-adic digit parallel fashion with a quadratic rate of convergence.

6. Solution of a system of linear equations by linear convergence

We now briefly consider the problem of determining the solution to a system of linear equations iteratively.

Let $Ax=b$ be a system of linear equations such that $\det A \bmod p \neq 0$, p being a prime. Let $A=A_1 \bmod p$ and $b_1=b \bmod p$. We first solve $A_1 x^{(1)}=b_1 \bmod p$ by Gaussian elimination (say) and thereafter use the iterative scheme

$$x^{(k+1)} = (p A_1^{-1} M x^{(k)} + A_1^{-1} b) \bmod p^{k+1} \quad (k=1,2,\dots)$$

where $A=A_1-p M$ and M is the error matrix. We can easily show by induction that

$$(Ax^{(k)} - b) \bmod p^k = 0.$$

Then, our algorithm is formally:

Step 1 Solve $A_1 x^{(1)}=b_1 \bmod p$.

Step 2 Use $x^{(k+1)}=(p A_1^{-1} M x^{(k)} + A_1^{-1} b) \bmod p^{k+1}$ to obtain the next iterate.

Step 3 If $\text{EUCLID}(x^k) = \text{EUCLID}(x^{k+1})$ stop; else go to 2.

Remark

Note that this scheme for the solution of linear equations has only a linear order convergence. However, it has the advantage of using only matrix-vector multiplications unlike the Newton iterative scheme where matrix-matrix multiplications are involved.

7. Concluding remarks

(i) The scheme of formula (3) gives rise to quadratic convergence. It is possible to use schemes having higher-order convergence. The following scheme, for example,

$$B_3^n = B_3^{n-1} (I + (I - B_3^{n-1}) (2I - AB_3^{n-1})) \text{ mod } p^{3^n} \quad (10)$$

has cubic convergence.

(ii) We have assumed throughout that $\det A \text{ mod } p \neq 0$, but in actual computation we cannot assume this a priori. We can keep choosing one prime after another until we succeed; but this is very expensive computationally. It would be better to use the method of rank 1 update, which is as follows:

We apply our algorithm to $A+V$ instead of A where

$$V = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \quad [b_1, b_2, \dots, b_n] = ab^t \quad \begin{array}{l} \text{is arbitrarily} \\ \text{chosen.} \end{array} \quad (11)$$

Finally, we use the formula

$$A^{-1} = (A+V)^{-1} + \frac{(A+V)^{-1} V (A+V)^{-1}}{1 - b^t (A+V)^{-1} a} \quad (12)$$

to retrieve the actual inverse. This method always succeeds except when $A^{-1} = 0$ over \mathbb{Z} and $A \text{ mod } p = 0$.

(iii) It is possible to extend the scope of our algorithm for the determination of the g-inverse of a singular matrix.

(iv) The algorithm determines all the elements of the inverse matrix simultaneously in p-adic digit parallel fashion with a quadratic or higher-order convergence rate [13].

- (v) In solving a system of linear equations, we note that we have split the matrix A in a very special way, namely, $A = A_1 - p M$. We could try splitting it as in the Jacobi, Gauss-Seidel or SOR method [3]; but unfortunately, the convergence in our sense is not realizable in these cases.
- (vi) We can invert polynomial matrices whose elements are in $\mathbb{Z}[x]$ [2] by constructing the inverses of the matrices $Z[x] \bmod p_i$ for several primes p_i and then using the Chinese Remainder Theorem to construct the actual inverse [1].

i	(u_i, u'_i)	(a_i, b_i)	q_i	(t_i, t'_i)
0	$(p^r, 0)$	$(w, 1)$	$[u_0/w]$	$(u_0 - a_0 q_0, u'_0 - b_0 q_0)$
1	$(w, 1)$	(t_0, t'_0)	$[u_1/a_1]$	$(u_1 - a_1 q_1, u'_1 - b_1 q_1)$
2	(t_0, t'_0)	(t_1, t'_1)	$[u_2/a_2]$	$(u_2 - a_2 q_2, u'_2 - b_1 q_2)$
.
k	(u_k, u'_k)	$(1, w^{-1})$	$[u_k/a_k]$	$(0, (-1)^{k+1} p^r)$

Table 1
Euclidean Algorithm

i	(u_i, u'_i)	(a_i, b_i)	q_i	(t_i, t'_i)
0	(625, 0)	(448, 1)	1	(177, -1)
1	(448, 1)	(177, -1)	2	(94, 3)
2	(177, -1)	(94, 3)	1	(83, -4)
3	(94, 3)	(83, -4)	1	(11, 7)
4	(83, -4)	(11, 7)	7	(6, -53)
5	(11, 7)	(6, -53)	1	(5, 60)
6	(6, -53)	(5, 60)	1	(1, -113)
7	(5, 60)	(1, -113)	5	(0, 625)

Table 2
Example of Euclidean algorithm

References

1. E. V. Krishnamurthy, Exact inversion of a rational polynomial matrix using finite field transforms, SIAM J. Appl. Math. 35, 453-464, 1978.
2. E. V. Krishnamurthy, T. M. Rao, and K. Subramanian, Residue arithmetic algorithms for computing g-inverses of matrices, SIAM J. Num. Anal. 13, 155-171, 1976.
3. J. Stoer and R. Bulirsch, An Introduction to Numerical Analysis, Springer-Verlag, 1981.
4. E. V. Krishnamurthy, Economical iterative and range-transformation schemes for division, IEEE Trans. on Computers, Vol. C-20, 470-472, 1971.
5. E. V. Krishnamurthy, T. M. Rao and K. Subramanian, Finite segment p-adic number systems with applications to exact computation, Proc. Indian Acad. Sci., Vol. 81A, pp. 58-79, February 1975.
6. E. V. Krishnamurthy, T. M. Rao, and K. Subramanian, p-adic arithmetic procedures for exact matrix computation, Proc. Indian Acad. Sci., Vol. 82A, pp. 165-175, November 1975.
7. E. V. Krishnamurthy, Matrix processors using p-adic arithmetic for exact linear computations, IEEE Trans. Computers Vol. C-26, pp. 633-639, July 1977.
8. R. T. Gregory, Error-Free Computation, Robert E. Krieger Pub. Co., Huntington, NY, 1980.
9. R. T. Gregory, The use of finite segment p-adic arithmetic for exact computation, BIT, Vol. 21, pp. 282-300, September 1978.
10. D. E. Knuth, The Art of Computer Programming 2: Semi-numerical algorithms, Addison-Wesley, Reading, MA, 1980.
11. E. V. Krishnamurthy, On the conversion of Hensel codes to Farey rationals, IEEE Trans. Computers (in press).
12. A. Ya. Khinchin, Continued Fractions, The University of Chicago Press, Chicago, IL, 1964.
13. G. Rodrigue, Parallel Computations, Academic Press, NY, 1982.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) ERROR-FREE PARALLEL HIGH-ORDER CONVERGENT ITERATIVE MATRIX INVERSION BASED ON p-ADIC APPROXIMATION		5. TYPE OF REPORT & PERIOD COVERED Technical
7. AUTHOR(s) E. V. Krishnamurthy		6. PERFORMING ORG. REPORT NUMBER TR-1529
		8. CONTRACT OR GRANT NUMBER(s) AFOSR-77-3271
9. PERFORMING ORGANIZATION NAME AND ADDRESS Computer Vision Laboratory Computer Science Center University of Maryland College Park, MD 20742		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS C-1142F 2384/1
11. CONTROLLING OFFICE NAME AND ADDRESS Math. & Info. Sciences, AFOSR/NM Rolling AFB Washington, DC 20332		12. REPORT DATE November 1982
		13. NUMBER OF PAGES 18
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Parallel computation Matrix inversion p-adic approximation		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) The Newton-Schultz iterative scheme is reformulated in an algebraic setting to compute the exact inverse of a matrix (or the solution of a linear system of equations) over the ring of integers, with a high order of convergence, by using a finite segment p-adic representation of a rational. This method is divergence-free; it starts with the inverse of a given matrix over a finite field (called the priming step) and then iterates successively to construct, in parallel, the p-adic approximants (Hensel Codes) of the rational		

D
FI
6-